

Report of the President of the United States  
on the  
Status of Federal Critical Infrastructure  
Protection Activities

January 2001

# Table of Contents

<b>Preface</b>	<b>iv</b>
<b>I. OVERVIEW</b>	<b>1</b>
<b>Introduction</b>	<b>2</b>
<b>The Problem and Challenges</b>	<b>2</b>
<b>Presidential Decision Directive 63</b>	<b>3</b>
<b>A Roadmap to the Report</b>	<b>7</b>
<b>II. STATUS OF PUBLIC-PRIVATE PARTNERSHIP BUILDING EFFORT</b>	<b>9</b>
<b>A. Introduction</b>	<b>10</b>
<b>B. Sector Partnerships</b>	<b>11</b>
1. Banking And Finance	11
2. Energy	13
3. Information and Communications (I&C)	16
4. Transportation (DOT)	20
5. Water Supply	20
6. Emergency Fire Services and Continuity Of Government	22
7. Emergency Law Enforcement	23
8. Public Health Services Sector	24
<b>C. Cross-Sector Partnerships</b>	<b>24</b>
1. National Outreach and Awareness Partnerships	24
2. Law Enforcement Information Sharing: Indications and Warning Partnerships	28
<b>III. STATUS OF INTERNAL AGENCY CIP PLANNING</b>	<b>30</b>
<b>A. Federal Agency Roles and Responsibilities</b>	<b>31</b>
<b>B. Cabinet Departments</b>	<b>33</b>
1. Department of Commerce	33
2. Department of Defense	34
3. Department of Education	38
4. Department of Energy	40
5. Department of Health and Human Services	41
6. Department of Housing and Urban Development	42
7. Department of Interior	43

8. Department of Justice	43
9. Department of Labor	46
10. Department of State	47
11. Department of Transportation	50
12. Department of Treasury	52
13. Department of Veterans Affairs	54
<b>C. Federal Agencies</b>	<b>55</b>
1. Environmental Protection Agency	55
2. Federal Emergency Management Agency	56
3. General Services Administration	57
4. National Aeronautics and Space Administration	60
5. National Science Foundation	61
6. National Security Agency	62
7. Nuclear Regulatory Commission	64
8. Social Security Administration	65
<b>D. Best Practices and Standards</b>	<b>66</b>
1. Office of Management and Budget	66
2. National Institute of Standards & Technology	69
3. National Information Assurance Partnership (NIAP)	71
4. Intelligence Issues	71
<b>IV. EDUCATION &amp; TRAINING</b>	<b>73</b>
<b>V. CRITICAL INFRASTRUCTURE PROTECTION R&amp;D</b>	<b>78</b>
<b>A. Information and Communication</b>	<b>79</b>
<b>B. Banking and Finance</b>	<b>80</b>
<b>C. Energy</b>	<b>81</b>
<b>D. Transportation</b>	<b>83</b>
<b>E. Vital Services</b>	<b>85</b>
<b>F. Interdependencies</b>	<b>87</b>
<b>G. International R&amp;D</b>	<b>88</b>
<b>VI. INDUSTRY INTERIM PROGRESS REPORTS</b>	<b>91</b>
<b>A. Banking and Finance Sector</b>	<b>93</b>
<b>B. Electric Power Sector</b>	<b>99</b>
<b>C. Oil and Gas Sector</b>	<b>103</b>

<b>D. Partnership for Critical Infrastructure Security</b>	<b>121</b>
<b>VII. APPENDICES</b>	<b>158</b>
<b>A. Department of Defense</b>	<b>159</b>
National Security Agency	173
<b>B. Department of Energy</b>	<b>179</b>
<b>C. Social Security Administration</b>	<b>183</b>
<b>D. Index to Acronyms</b>	<b>195</b>

# Preface

This congressionally requested report provides the status at the beginning of 2001 of Federal Government and industry programs on cyber security. Departments submitted their own input for this report.

In recent years, there has been a growing recognition that the new economy is dependent upon Information Technology (IT) networks and systems, which are vulnerable to malicious disruption. As a result, there have been Federal Government efforts to fix federal systems and work with industry to secure critical information systems.

The potential problems are even more significant than first thought. More of the American economy has become dependent upon IT systems. Those who have the skills and tools to disrupt our networks and systems have also increased, in numbers and capability. Malicious individuals, criminal groups, and nation states present significant threats to U.S. information systems.

Over the next three years, traditional telephony networks and data transmission systems are converging with the Internet into a single formatted, digital, packet-switched network. Fiber optic lines and new optical switches will create an expanding optical core for the new networks. Finally, wireless devices linked to the Internet and the new converged, fiber networks will replace a multiplicity of today's devices (cell phones, PDAs, pagers, notebook computers, and credit cards). While on-going efforts continue to increase security on the nation's current IT systems, government and industry must insure that security is designed into next generation networks.

In recognition of the growing threats and the new opportunities in the next generation National Information Infrastructure, the Federal Government has:

- Overcome the mistrust between the government and critical industry groups.
- Created effective public-private partnerships.
- Greatly increased the security of the Defense Department's networks and laid out a plan for continued improvement.
- Established information sharing and analysis centers in some key industries and some Federal Government agencies running major networks.
- Initiated a cyber security scholarship program and is working with higher education and industry to address the shortage of trained information technology personnel in the Federal Government.
- Begun establishing a baseline for standards and a system to enforce them within Federal agencies.
- Established initial requirements for a national system to identify, limit, and recover from significant information warfare attacks and malicious hacks.

- Initiated discussions with government and industry on interdependencies across sectors, the operation of the new networks, and the requirement for the converged telephony/IP system to be designed with enhanced security.
- Encouraged partnerships with industry to more sectors and continued stimulating market forces (audit, insurance, and legal) to reduce vulnerabilities in privately owned and operated critical infrastructures.

Additional accomplishments are enumerated in the report.

Achievements to date are notable, but there is still work to do. At present, there is no government-wide means for identifying critical systems and their vulnerabilities and then fixing them. Nor is there a government-wide means of tracking the progress of departments in achieving specified goals. The General Accounting Office of Congress has provided a useful review of cyber security of the departments, but has been able to examine only a few agencies annually.

The IT Revolution of the last eight years has transformed our nation for the better. Economic growth, better government service and efficiency, and a stronger defense are all possible in the years ahead if we continue to give high priority to securing cyber space.

## **I. OVERVIEW**

# I. OVERVIEW

## **Introduction**

This report is submitted pursuant to the requirement in Presidential Decision Directive 63 (PDD-63) for the National Coordinator to provide an annual report on the implementation of PDD-63 to the President and heads of departments and agencies.

The first part of this introductory section briefly discusses the types of threats posed by the evolution of Information Technology (IT) and related trends. The second part provides an overview of PDD-63 and the government structures created to implement it. The last part sets forth a roadmap for the rest of the report.

## **The Problem and Challenges**

### *Dependency, Vulnerability, and Threat*

During the past decade, our increasing use of automated systems and devices has stimulated unprecedented prosperity. At the same time, the maturing of the Information Age has also led to new types of threats and vulnerabilities.

America's critical infrastructures are the foundation of our economy, national security, and quality of life. The functioning of critical parts of our economy, government, and national security now depend upon computer-managed information networks. Our infrastructures increasingly rely on interconnected information systems and networks. This development creates a new dimension of vulnerability which, when combined with an emerging array of threats, poses a new set of risks to the nation's security and economic power. Potential adversaries—be they nation-states, cyber-terrorist groups, criminal organizations, or disgruntled insiders—can easily develop effective cyber-attack capabilities to exploit this vulnerability.

Currently available hacker exploits permit an attacker to conceal points of origin by hopping through several intermediate way stations in cyber space—crossing and re-crossing national borders in the process. These capabilities make identification of an attacker a daunting challenge. Established terrorist groups are likely to view attacks against information systems and critical infrastructures as an attractive way to strike at government, commercial, and industrial targets with little risk of detection.

In short, unlike the familiar national-security threats of the past century, these cyber threats can come from anywhere. They can originate from any location, affect systems anywhere in the world, disguise their origins and travel routes, and do it all instantaneously. Without firing a shot or crossing a border, an enemy with the right tools and techniques can damage our economy and slow down our military.

### *The Need for Effective Public-Private Partnerships*

Unlike other forms of national security threats, the Federal Government cannot address these threats to critical infrastructures in isolation. Most of our critical infrastructures are privately owned and operated. Many of the owners and operators are business competitors. The protection of our critical

infrastructures, therefore, necessarily requires a shared responsibility and partnership between owners and operators and the government.

Effective critical infrastructure protection (CIP), and in particular the provision of adequate cyber-security, really requires a comprehensive system approach that consists of business processes, cultures, and policies, as well as access to appropriate technical tools and trained personnel.

Failures of infrastructure and cyber-security can directly harm business operations by affecting their bottom lines, eroding consumer confidence, and disrupting operations. Serious problems can lead to major disruptions throughout the economy.

Furthermore, infrastructure protection by its nature cannot be static. In today's high-speed business world, core business processes and technology are constantly changing in order to create competitive advantages and efficiency. It is not always clear which drives which. The pace of change is measured in months rather than years. Consequently, assuring the safety of the information systems that underlie our critical infrastructures will mean integrating an on-going concern for security into the business decisions of managers as well as technologists. That process will have to start at the highest levels of management.

### **Presidential Decision Directive 63**

On May 22, 1998, President Clinton issued PDD-63 to achieve and maintain the capability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services; and
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services.

To achieve these ends, the PDD-63 articulates a strategy of:

- creating a public-private partnership to address the problem of information technology security;
- raising awareness of the importance of cyber security in the government and in the private sector;
- stimulating market forces to increase the demand for cyber security and to create standards or best practices;
- funding or facilitating research into new information technology systems with improved security inherent in their design;
- working with higher educational facilities to increase the number of students specializing in cyber security;
- helping to prevent, mitigate, or respond to major cyber attacks by building an information sharing system among government agencies, among corporations, and between Government and industry.

The government's basic approach to CIP, as reflected in PDD-63, has been built around a strong policy preference for consensus-building and voluntary cooperation rather, than regulatory actions. In an economy as complex as ours, and with technology changing as quickly as it is, cooperation offers the best and surest way to achieve our shared goals in this emerging area. However, the government's approach also recognizes the need for coordinated actions to improve its internal defenses and the nation's overall posture against these new threats.

---

## **Section I: Overview**

---

For this reason, implementation of PDD-63 has proceeded along two simultaneous policy tracks:

- To establish an effective system of partnership arrangements with the private industry within each infrastructure sector, across all the infrastructure sectors, and with other key stakeholders, including the audit, insurance and investment communities, to raise awareness and to catalyze market driven activities and solutions.
- To improve the government's own systems and plans for critical infrastructure assurance, including the development of internal plans, improved recruitment, education and training for Federal personnel, and a comprehensive program of research and development in these areas.

PDD-63 addresses the unique structural challenges that CIP poses for the Federal Government.

“No office, organization or individual within the Federal Government has overall responsibility for infrastructure protection or policy. This is not surprising as there was little need for a national focal point when infrastructures were largely independent discrete, insulated by geography and protected by military defenses. Today, however, the interdependent, interconnected nature of the infrastructures, and their exposure to cyber and other threats, creates a real need for a single point of focus. To support this, a federal framework needs to be created, working in conjunction with state and local governments and the private sector, to implement a national policy on infrastructure protection.<sup>1</sup>”

To meet these challenges, PDD-63 has created new organizational structures to compliment those already in place:

- The **National Coordinator for Security, Critical Infrastructure and Counter-Terrorism** at the White House National Security Council (NSC) staff. The National Coordinator serves as a spokesperson for the issue of cyber security and provides oversight for the implementation of PDD-63 and the National Plan.
- The **Critical Infrastructure Assurance Office (CIAO)**, an interagency office housed at the Commerce Department, assists in the coordination of the Federal Government's initiatives on critical infrastructure protection. It has three basic missions. First, it coordinates the drafting of the National Plan for Information Security Protection. Version 1.0 of the plan was issued by President Clinton in January 2000. Second, it assists Federal agencies in analyzing their critical infrastructure dependencies and interdependencies. CIAO has initiated Project Matrix whereby it is helping civilian agencies to identify those assets that are key to the fulfillment of their national security, economic stability, and critical public health and safety responsibilities. Finally, it coordinates national outreach, education and awareness efforts. The CIAO has been the catalyst in the creation by private-sector companies of the Partnership for Critical Infrastructure Security. In implementing its mandates, the CIAO is focusing on issues that cut across industry sectors (and are not the existing responsibility of agencies). In this way, it helps to ensure a coherent and cohesive U.S. approach to the protection of our critical infrastructures.

---

<sup>1</sup> “Critical Foundations –Protecting America’s Infrastructures;” The Report of the President’s Commission on Critical Infrastructure Protection, page 50.

- The **National Infrastructure Protection Center (NIPC)**, an interagency office housed at the Federal Bureau of Investigation (FBI), serves as a threat coordination center focusing on threat warnings, vulnerabilities, and law enforcement. The Center is staffed by a mix of FBI employees and detailees from other Federal agencies. In addition, the Center has had state law enforcement officials detailed on a rotating basis and hosts representatives from the United Kingdom and Canada. The center has a vital role in collecting and disseminating information from all relevant sources. The NIPC sanitizes law enforcement for inclusion into analyses and reports that it provides, in appropriate form, to relevant federal, state, and local agencies, owners and operators of critical infrastructures, private sector information sharing and analysis entities, and to the public. The NIPC also issues attack warnings or alerts to increases in threat condition to private sector owners and operators. In the first ten weeks of FY 2001 the NIPC has issued eight warnings. Each of the 56 FBI field offices has agents assigned to infrastructure protection matters, to include investigating computer intrusions, denials of service, and virus cases; performing outreach initiatives; creating computer crime task forces with state and local law enforcement; training for computer crime investigators; developing an intelligence base; and supporting significant FBI cases that require computer investigative expertise.
- For each infrastructure sector that could be a target for significant cyber or physical attacks, a single U.S. Government Department or Agency serves as the Lead Agency for liaison. Each Agency listed as a Lead Agency for a particular sector of the critical infrastructure will also designate a Sector Liaison Official to direct efforts in that sector. PDD-63 sector and Lead Agency designations are as follows:

<b>Critical Infrastructure Sector</b>	<b>Lead Agency</b>
Information and Communications	Commerce
Banking and Finance	Treasury
Water Supply	Environmental Protection Agency
Aviation, Highways, Mass Transit, Pipelines, Rail, Waterborne Commerce	Transportation
Emergency Law Enforcement Services	Justice/FBI
Emergency Fire Service, Continuity of Government Services	Federal Emergency Management Agency
Public Health Services	Health and Human Services
Electric and Power, Oil and Gas Production and Storage	Energy
Federal Government	General Services Administration

- The **Sector Liaison Officials** work closely with the National Coordinator on the Critical Infrastructure Coordinating Group (CICG), the interagency committee analyzing critical infrastructure policy issues and developing policy recommendations for the Cabinet-level Principals Committee.

- The **Critical Infrastructure Coordination Group** is the primary interagency coordination body for the implementation of PDD-63. CICG membership is comprised of senior policy level (Assistant Secretary or higher) officials and includes the Sector Liaisons, Functional Coordinators of the Lead Agencies, as well as representatives from other relevant Departments and Agencies, including the National Economic Council. The National Coordinator chairs the CICG. Where appropriate, the CICG is assisted by existing policy structures.
- Functional areas that have no private sector counterparts (defense, intelligence, foreign affairs, law enforcement, and research and development) are also represented on the CICG by Special Functional Coordinators. These are:

Special Functional Coordinators	
Foreign Affairs	State Department
National Defense	Defense
Foreign Intelligence	Central Intelligence Agency
Law Enforcement and Internal Security	Justice/FBI
Research and Development	Office of Science and Technology Policy

- The **Cyber Incident Steering Group (CISG)** and **Cyber Incident Working Group (CIWG)** are both sub-groups of the CICG that convene to coordinate policy and operational issues in the event that extensive cyber-related disruptions to critical systems occur. The CISG is chaired by the National Coordinator and provides policy guidance to the CIWG and recommendations to the NSC Principals. The CIWG, chaired by the Director of the NIPC, coordinates operational and law enforcement matters among the Federal Agencies during a cyber event. The work of these two bodies does not derogate existing agency authorities for law enforcement, intelligence, or national defense and ensures proper interagency coordination.
- The **Chief Information Officers Council (CIO Council)**, comprised of Federal CIOs, works to protect the privacy and availability of the data on Federal information systems. Its **Subcommittee on Security, Privacy, and Critical Infrastructure** ensures implementation of security practices within the Federal Government in order to prevent interruption of government services, maintain privacy, and protect sensitive and national security classified information. Through these efforts, senior executives within the government are kept abreast of developing information security issues and exchange information on techniques for dealing with IT security risks.
- The **Joint Telecommunications Resources Board (JTRB)** assists the Director of the Office of Science and Technology Policy (OSTP) in the Executive Office of the President in the exercise of authorities over the National Communications System (NCS) in non-wartime emergency situations. The National Communications Center (NCC), a component of the NCS, is comprised of private sector companies and supported by OSTP and the JTRB. It is a key element of the Federal telecommunications infrastructure and represents a strong model of public-private partnerships.

- The **National Security Telecommunications and Information Systems Security Committee (NSTISSC)** was established in 1990 to provide a forum for the discussion of policy issues and to provide operational guidance for the protection of national security systems. Its members include a broad range of civilian and military agencies.
- The **National Information Assurance Partnership (NIAP)<sup>SM</sup>** is a U.S. Government initiative designed to meet the security-testing needs of both information technology producers and users. NIAP is a collaboration of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The partnership combines the extensive IT security experience of both agencies. The program is intended to foster the availability of objective measures and test methods for evaluating the quality of IT security products. In addition, it is designed to foster the development of commercial testing laboratories that can provide the types of testing and evaluation services, which will meet the demands of both producers and users.
- The **Federal Computer Incident Response Capability (FedCIRC)** is the central coordination and analysis facility dealing with computer security related issues affecting the civilian agencies and departments of the Federal Government. FedCIRC's incident response and advisory activities bring together elements of the Department of Defense, law enforcement, the Intelligence Community, academia and computer security specialists from Federal civilian agencies and departments, forming a multi-talented virtual security team.
- The **Federal Cyber Services (FCS)** training and education initiative is an element of the National Plan and is designed to ensure an adequate supply of highly skilled Federal information system security specialists. The "Scholarship for Service" program, a component of FCS, was recently funded for FY 2001. The National Science Foundation and the Office of Personnel Management administer the program jointly. The program offers scholarships for up to two years in exchange for a commitment to an equal amount of service to the Federal Government.

## **A Roadmap to the Report**

The remainder of the Report is organized as follows:

- *Section 2* reports on the government's efforts to foster effective public-private partnerships, beginning with a discussion of the sector-level programs sponsored by Federal lead agencies and concluding with a review of cross-sector partnership efforts, that include national education and awareness partnerships implemented by the CIAO and law enforcement information sharing/indications and warning partnerships implemented by the NIPC.
- *Section 3* reports on internal efforts within the Federal government to secure our internal systems and infrastructures. The section begins with a review of the programs at Cabinet-level departments (listed in alphabetical order). Later sub-sections review similar programs at Federal agencies and the government's overall efforts to promote CIP best practices and standards.
- *Section 4* reports on CIP education and training initiatives. These initiatives have several purposes: to increase the supply of trained IT security staff within Federal agencies, build academic programs in the fields of cyber-security and infrastructure protection, and increase awareness among educators and students of the need for good cyber-security practices.

---

## **Section I: Overview**

---

- *Section 5* reviews CIP research and development programs. These programs are discussed on a sector-by-sector basis.
- *Section 6* contains progress reports independently prepared and voluntarily submitted for inclusion in this document by several private industry sectors and partnerships. We have offered private industry the opportunity to provide its own perspective on the state of CIP and related issues. These reports have been included as received from the respective industry sectors and partnerships and reflect their independent views.